

ANSWER TO A QUESTION ON A -GROUPS, ARISEN FROM THE STUDY OF STEINITZ CLASSES

ALESSANDRO COBBE AND MAURIZIO MONGE

ABSTRACT

In this short note we answer to a question of group theory from [2]. In that paper the author describes the set of realizable Steinitz classes for so-called A' -groups of odd order, obtained iterating some direct and semidirect products. It is clear from the definition that A' -groups are solvable A -groups, but the author left as an open question whether the converse is true. In this note we prove the converse when only two prime numbers divide the order of the group, but we show it to be false in general, producing a family of counterexamples which are metabelian and with exactly three primes dividing the order. Steinitz classes which are realizable for such groups in the family are computed and verified to form a group.

1. INTRODUCTION

Let K/k be an extension of number fields with rings of integers \mathcal{O}_K and \mathcal{O}_k respectively. Then there exists an ideal I of \mathcal{O}_k such that

$$\mathcal{O}_K \cong \mathcal{O}_k^{[K:k]-1} \oplus I$$

as \mathcal{O}_k -modules and the ideal I is determined up to principal ideals. Its class in the ideal class group $\text{Cl}(\mathcal{O}_k)$ of \mathcal{O}_k is called the Steinitz class of the extension and is denoted by $\text{st}(K/k)$. For a fixed number field k and a finite group G one can consider the set of classes which arise as Steinitz classes of tame Galois extensions with Galois group G , i.e. the set

$$\text{R}_t(k, G) = \{x \in \text{Cl}(k) : \exists K/k \text{ tame Galois, } \text{Gal}(K/k) \cong G, \text{st}(K/k) = x\}.$$

A description of $\text{R}_t(k, G)$ is not known in general, but there are a lot of results for some particular groups. These results lead to the conjecture that $\text{R}_t(k, G)$ is always a subgroup of the ideal class group, which however has not been proved in general. In [2] the author defines A' -groups in the following way and proves the above conjecture for all A' -groups of odd order.

Definition 1.1. *We define A' -groups inductively:*

- (1) *Finite abelian groups are A' -groups.*
- (2) *If \mathcal{G} is an A' -group and H is finite abelian of order prime to that of \mathcal{G} , then $H \rtimes_{\mu} \mathcal{G}$ is an A' -group, for any action μ of \mathcal{G} on H .*
- (3) *If \mathcal{G}_1 and \mathcal{G}_2 are A' -groups, then $\mathcal{G}_1 \times \mathcal{G}_2$ is an A' -group.*

Clearly (see [2, Proposition 1.2]) every A' -group is a solvable A -group, while it was asked whether the converse is true. In this short note we find a family of counterexamples for this. In the last section we show how the techniques from [2] can be applied also to the calculation of the realizable Steinitz classes for these groups, showing in particular that $\text{R}_t(k, G)$ is still a subgroup of the ideal class group, confirming the general conjecture.

2010 *Mathematics Subject Classification.* 20F16, Secondary: 11R33.

Key words and phrases. A -groups, Steinitz classes, solvable groups.

2. SOLVABLE A -GROUPS WHICH ARE NOT A' -GROUPS

We start showing a positive result when only two primes divide the order. See [5, 4] for general results about the A -groups.

Proposition 2.1. *An A -group G having order divisible by at most two different primes is an A' -group.*

Proof. Indeed, let G be an A -group with order divisible only by the primes p and q ; it is always solvable by Burnside Theorem. By Hall-Higman Theorem [4, Satz VI.14.16] a solvable A -group has derived length at most equal to the number of distinct prime divisors of the order, so in our case G has derived length at most 2 and G' is abelian. If the derived length is 1 then G is abelian, so we are reduced to consider the case of derived length exactly 2.

We will consider the unique subgroup K_p such that $K_p G' / G'$ is the p -Sylow of G / G' and $K_p \cap G'$ is the q -Sylow of G' and we will show it to be normal in G . Further by Schur-Zassenhaus Theorem it is an A' -group, being the semidirect product of an abelian q -group by an abelian p -group. Constructing analogously K_q , with p and q flipped, we have that $K_p \cap K_q = 1$, while $K_p K_q$ is all of G , so K_p and K_q are direct factors of G , since they are normal. Therefore G is isomorphic to $K_p \times K_q$ and consequently G is an A' -group by rule 3.

To construct K_p let's quotient out the q -Sylow S_q of G' , obtaining the group $\tilde{G} = G / S_q$. Its p -Sylow, \tilde{P} say, is clearly normal being the inverse image of the p -Sylow of G / G' , which is a p -group since we killed all the q -part of G' . So we have the exact sequence

$$1 \rightarrow \tilde{P} \rightarrow \tilde{G} \rightarrow \tilde{G} / \tilde{P} \rightarrow 1,$$

and furthermore \tilde{G}' is equal to G' / S_q being $S_q \subseteq G'$, and is contained in \tilde{P} being \tilde{G} / \tilde{P} abelian.

Now \tilde{G}' has a complementary factor in \tilde{P} which is invariant under the action by conjugation of the q -group \tilde{G} / \tilde{P} by [3, Theorem 2.3, Chap. 5], so let's assume $\tilde{P} = \tilde{G}' \times F_p$ say. Clearly F_p is a p -group which is normal in \tilde{G} , and $F_p \tilde{G}' / \tilde{G}'$ is the p -Sylow of $\tilde{G} / \tilde{G}' = G / G'$. So if we put K_p to be the preimage of F_p under the projection $G \rightarrow \tilde{G}$ we have that K_p is normal in G , $K_p G' / G'$ is the p -Sylow of G / G' , and $K_p \cap G'$ is the q -Sylow S_q of G' , being the preimage of $F_p \cap \tilde{G}' = 1$. \square

For any triple p, q, r of distinct primes we construct now a counterexample which is a metabelian group. For any integer n let C_n be the cyclic group on n elements.

Let a, b be integers such that

$$qr \mid p^a - 1, \quad pr \mid q^b - 1,$$

or equivalently such that $\text{ord}_{qr}^\times(p) \mid a$ and $\text{ord}_{pr}^\times(q) \mid b$. Let \mathbb{F}_{p^a} and \mathbb{F}_{q^b} respectively be the fields with p^a and q^b elements, then the multiplicative groups $\mathbb{F}_{p^a}^\times$ and $\mathbb{F}_{q^b}^\times$ act naturally as automorphisms on the additive groups $\mathbb{F}_{p^a}^+$ and $\mathbb{F}_{q^b}^+$. If $\phi : C_q \hookrightarrow \mathbb{F}_{p^a}^\times$ and $\psi : C_p \hookrightarrow \mathbb{F}_{q^b}^\times$ are embeddings we can consider the semidirect products

$$H_1 = \mathbb{F}_{p^a}^+ \rtimes_\phi C_q, \quad H_2 = \mathbb{F}_{q^b}^+ \rtimes_\psi C_p.$$

Let's also consider embeddings $\rho_1 : C_r \hookrightarrow \mathbb{F}_{p^a}^\times$ and $\rho_2 : C_r \hookrightarrow \mathbb{F}_{q^b}^\times$, since $\mathbb{F}_{p^a}^\times$ and $\mathbb{F}_{q^b}^\times$ are abelian groups the actions induced by C_r on $\mathbb{F}_{p^a}^+$ and $\mathbb{F}_{q^b}^+$ commute with those of C_q and C_p , so ρ_1, ρ_2 induce an action of C_r on H_1 and H_2 which is trivial on C_p and C_q .

We define

$$G = (H_1 \times H_2) \rtimes_{\rho_1, \rho_2} C_r,$$

where C_r acts on H_i via ρ_i , for $i = 1, 2$.

Proposition 2.2. *G is a metabelian A -group which is not an A' -group.*

Proof. Indeed, G is metabelian because $\mathbb{F}_{p^a}^+ \times \mathbb{F}_{q^b}^+$ is a normal abelian subgroup with abelian quotient, isomorphic to $C_q \times C_p \times C_r$.

To show that G cannot be obtained applying rule 2 in the inductive definition of the A' -groups we prove that no Sylow subgroup is normal. Since $(r, p) = 1$, a p -Sylow P is contained in $H_1 \times H_2$, and if normal then $H_2 \cap P$ would be normal in H_2 too, but C_p in $\mathbb{F}_{q^b}^+ \rtimes C_p$ is clearly not normal or it would be complemented by the normal subgroup $\mathbb{F}_{q^b}^+$ and H_2 would be abelian, which is not the case. The same holds for the q -Sylow of H_1 , and similarly C_r cannot be normal unless $G = (H_1 \times H_2) \times C_r$ and all elements of order r would be contained in the center of G , which is not the case.

To conclude we just need to show that G is not a direct product, so it also cannot be obtained applying rule 3. Suppose $G = G_1 \times G_2$, then exactly one of G_1, G_2 has order divisible by r , so assume $r \mid |G_1|$, and we have that G_1 contains all r -Sylow subgroups, so in particular $C_r \subset G_1$. Then G_2 is contained in the centralizer of C_r , that considering the definition of G we can see to be equal to $C_p \times C_q \times C_r$. But $r \nmid |G_2|$, and if $p \mid |G_2|$ we would have $C_p \subset G_2$ and C_p would be the p -Sylow, and hence a characteristic subgroup, of G_2 , and consequently normal in G , which is absurd. Since we can prove similarly that $q \nmid |G_2|$ we obtain $G_2 = 1$. \square

We remark that some of the smallest counterexamples are those obtained putting the $(p, q, r; a, b)$ equal to $(5, 2, 3; 2, 4)$ and $(13, 3, 2; 1, 3)$. The groups produced have orders respectively 12000 and 27378, and are already a bit too far away to be found in a brute-force computer search, as was performed by the author of [2].

Note that we have the exact sequence

$$1 \rightarrow \mathbb{F}_{p^a}^+ \rightarrow G \rightarrow (C_q \times H_2) \rtimes C_r \rightarrow 1,$$

we prove now a Lemma which will be of use later.

Lemma 2.3. *Every group fitting as central term in the above exact sequence, with the given action of the quotient on the kernel, is uniquely determined.*

Proof. Indeed, let H be the subgroup of index r of G which is the preimage of $C_q \times H_2$ in G . Note that the p -Sylow of H is abelian being C_p cyclic and with trivial action on $\mathbb{F}_{p^a}^+$, so H is an A -group and an A' -group by Proposition 2.1.

The group C_q acts onto $\mathbb{F}_{p^a}^+$ by conjugacy without fixed points except 0, and hence its preimage in G is a group whose derived subgroup is all of $\mathbb{F}_{p^a}^+$ being a direct complement to 0 by [3, Theorem 2.3, Chap. 5], so we have $\mathbb{F}_{p^a}^+ \subset H'$. Consequently H' is the preimage of the derived subgroup of $C_q \times H_2$, which is $\mathbb{F}_{q^b}^+$ being $H_2 \cong \mathbb{F}_{q^b}^+ \rtimes C_p$ with C_p acting again on $\mathbb{F}_{q^b}^+$ without fixed points except 0; in particular we have $H' \cong \mathbb{F}_{q^b}^+ \times \mathbb{F}_{p^a}^+$.

On the other hand the preimage of C_q is isomorphic to the semidirect product $\mathbb{F}_{p^a}^+ \rtimes_{\phi} C_q = H_1$ by Schur-Zassenhaus Theorem, and is exactly the factor K_q of Proposition 2.1 applied to H , because K_q is characterized as the group having intersection with the derived subgroup H' which is its p -Sylow $\mathbb{F}_{p^a}^+$, and such that $K_q H' / H'$ is the q -Sylow C_q of $H / H' \cong C_q \times C_p$.

Consequently the preimage of C_q is a direct factor of H . Its complementary factor K_p is isomorphic to H_2 , and mapped to H_2 in the exact sequence, so H is isomorphic to $H_1 \times H_2$. Since H is certainly complemented by Schur-Zassenhaus Theorem, and the H_1 and H_2 subgroups are produced in the proof of Proposition 2.1 in a canonical way so the decomposition is certainly C_r -invariant, we have that G is isomorphic to $H \rtimes_{\rho_1, \rho_2} C_r$, and it is the group we defined in the above construction. \square

3. REALIZABLE STEINITZ CLASSES

A natural question that arises having constructed these solvable A -groups which are not A' -groups is whether the techniques of [2] can be used to compute the corresponding realizable Steinitz classes.

Since there are some complications in the case of groups of even order, we will assume that p, q, r are all odd prime numbers. Nevertheless we remark that, in the even case, for these particular groups it is possible to use the results in [1] to calculate the realizable Steinitz classes.

We will use the notation and the terminology from [2]. Clearly $(C_q \times H_2) \rtimes C_r$ is an A' -group of odd order and so by Theorem 3.23 we know that $R_t(k, (C_q \times H_2) \rtimes C_r)$ is a group and that $(C_q \times H_2) \rtimes C_r$ satisfies some other properties which are summarized in [2, Definition 3.15] by the notion of good group. Further [2, Theorem 3.19] can be used to have an explicit description of $R_t(k, (C_q \times H_2) \rtimes C_r)$.

Proposition 3.1. *Let p, q, r be odd prime numbers, let G be defined as in the previous section and let k be a number field. Then*

$$R_t(k, G) = \prod_{\tau \in \mathbb{F}_{p^a}^+ \setminus \{0\}} W(k, E_{k, \mu, \tau})^{\frac{p-1}{2} \frac{|G|}{p}} R_t(k, (C_q \times H_2) \rtimes C_r)^{p^a}$$

where μ is the action of $(C_q \times H_2) \rtimes C_r$ on $\mathbb{F}_{p^a}^+$, $E_{k, \mu, \tau}$ is the fixed field of $G_{k, \mu, \tau}$ in $k(\zeta_p)$,

$$G_{k, \mu, \tau} = \left\{ g \in \text{Gal}(k(\zeta_p)/k) : \exists g_1 \in \mathcal{G}, \mu(g_1)(\tau) = \tau^{\nu_{k, \tau}(g)} \right\}$$

and $g(\zeta_p) = \zeta_p^{\nu_{k, \tau}(g)}$ for any $g \in \text{Gal}(k(\zeta_p)/k)$.

In particular this proves that $R_t(k, G)$ is a group.

Proof. The inclusion

$$R_t(k, G) \supseteq \prod_{\tau \in \mathbb{F}_{p^a}^+ \setminus \{0\}} W(k, E_{k, \mu, \tau})^{\frac{p-1}{2} \frac{|G|}{p}} R_t(k, (C_q \times H_2) \rtimes C_r)^{p^a}$$

is given by [2, Proposition 3.13], using Lemma 2.3 of the previous section.

Now we want to prove the opposite inclusion. Let K/k be a tame G -Galois extension of number fields and let k_1 be the subfield of K fixed by the normal subgroup $\mathbb{F}_{p^a}^+$. Let \mathfrak{p} be a prime which ramifies in K/k , let $e_{\mathfrak{p}}$ be its ramification index in k_1/k and let $e_{\mathfrak{P}}$ be the ramification index in K/k_1 of a prime \mathfrak{P} of k_1 dividing \mathfrak{p} . Since the extension K/k is tame the inertia group must be cyclic, and in particular so are its p -Sylow subgroups. But since the p -Sylow subgroups of G have exponent p , it follows that p^2 does not divide $e_{\mathfrak{p}}e_{\mathfrak{P}}$. In particular $e_{\mathfrak{P}} \in \{1, p\}$ and p can not divide both $e_{\mathfrak{p}}$ and $e_{\mathfrak{P}}$; it follows that $\gcd(e_{\mathfrak{p}}, e_{\mathfrak{P}}) = 1$. Therefore by the same arguments of the proof of [2, Lemma 3.17] there exist $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in \mathbb{Z}$ such that

$$(e_{\mathfrak{p}}e_{\mathfrak{P}} - 1) \frac{|G|}{e_{\mathfrak{p}}e_{\mathfrak{P}}} = a_{\mathfrak{p}}(e_{\mathfrak{p}} - 1) \frac{|G|}{e_{\mathfrak{p}}} + b_{\mathfrak{p}}(e_{\mathfrak{P}} - 1) \frac{|G|}{e_{\mathfrak{P}}}.$$

Since $(C_q \times H_2) \rtimes C_r$ is a good group by [2, Theorem 3.22], the class of

$$\mathfrak{p}^{a_{\mathfrak{p}} \frac{e_{\mathfrak{p}} - 1}{2} \frac{|G|}{e_{\mathfrak{p}}}}$$

is in

$$R_t(k, (C_q \times H_2) \rtimes C_r)^{p^a}.$$

If $e_{\mathfrak{P}} = p$ then by [2, Lemma 3.14] the class of \mathfrak{p} is in $W(k, \mu, \tau)$, where $\tau \in \mathbb{F}_{p^a}^+ \setminus \{0\}$ generates the inertia group of \mathfrak{P} in K/k_1 . Hence in both cases $e_{\mathfrak{P}} = 1$ and $e_{\mathfrak{P}} = p$ the class of

$$\mathfrak{p}^{\frac{e_{\mathfrak{p}}e_{\mathfrak{P}} - 1}{2} \frac{|G|}{e_{\mathfrak{p}}e_{\mathfrak{P}}}}$$

is in

$$\prod_{\tau \in \mathbb{F}_{p^a}^+ \setminus \{0\}} W(k, E_{k,\mu,\tau})^{\frac{p-1}{2} \frac{|G|}{p}} R_t(k, (C_q \times H_2) \rtimes C_r)^{p^a}.$$

The Steinitz class of K/k is the class of the ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\frac{e_{\mathfrak{p}} e_{\mathfrak{p}} - 1}{2} \frac{|G|}{e_{\mathfrak{p}} e_{\mathfrak{p}}}},$$

where the product runs over the set of primes which ramify in K/k , and so the second inclusion follows. \square

REFERENCES

- [1] A. Cobbe. Steinitz classes of some abelian and nonabelian extensions of even degree. *J. Théor. Nombres Bordeaux*, 22(3):607–628, 2010.
- [2] A. Cobbe. Steinitz classes of tamely ramified galois extensions of algebraic number fields. *Journal of Number Theory*, 130(5):1129 – 1154, 2010.
- [3] D. Gorenstein. *Finite groups*. Chelsea Pub. Co., 1980.
- [4] B. Huppert. *Endliche Gruppen I*, volume 134 of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen*. Springer, 1967.
- [5] D. Taunt. On a -groups. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 45, pages 24–42. Cambridge Univ Press, 1949.